Redpaper

Axel Buecker
Koos Lodewijkx
Harold Moss
Kevin Skapinetz
Michael Waidner

Cloud Security Guidance

IBM Recommendations for the Implementation of Cloud Security

In this IBM® Redpapers™ publication, we provide a discussion about the IBM recommendations for the implementation of cloud security. To get started, let us begin with an introduction to cloud computing and cloud security in general.

Introduction to cloud computing

Cloud computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. Cloud resources can be rapidly deployed and easily scaled, with all processes, applications, and services provisioned *on demand*, regardless of the user location or device.

As a result, cloud computing gives organizations the opportunity to increase their service delivery efficiencies, streamline IT management, and better align IT services with dynamic business requirements. In many ways, cloud computing offers the *best of both worlds*, providing solid support for core business functions along with the capacity to develop new and innovative services.

> **Note:** As an added benefit, cloud computing enhances the user experience without adding to its complexity. Users do not need to know anything about the underlying technology or implementations.

Both public and private cloud models are now in use. Available to anyone with Internet access, public models include *Software as a Service* (SaaS) clouds, such as IBM LotusLive, *Platform as a Service* (PaaS) clouds, such as Amazon Web Services, and *Security and Data Protection as a Service* (SDPaaS) clouds, such as IBM Security Event and Log Management Services.

Private clouds are owned and used by a single organization. They offer many of the same benefits as public clouds, and they give the owner organization greater flexibility and control.

Furthermore, private clouds can provide lower latency than public clouds during peak traffic periods. Many organizations embrace both public and private cloud computing by integrating the two models into hybrid clouds. These hybrids are designed to meet specific business and technology requirements, helping to optimize security and privacy with a minimum investment in fixed IT costs.

Although the benefits of cloud computing are clear, so is the need to develop proper security for cloud implementations. In the following sections, we provide an overview of key security issues related to cloud computing, concluding with IBM recommendations on the implementation of cloud security. The recommendations are built on various information security frameworks and industry best practices.

Cloud security: the grand challenge

In addition to the usual challenges of developing secure IT systems, cloud computing presents an added level of risk because essential services are often outsourced to a third party. The *externalized* aspect of outsourcing makes it harder to maintain data integrity and privacy, support data and service availability, and demonstrate compliance.

In effect, cloud computing shifts much of the control over data and operations from the client organization to their cloud providers, much in the same way organizations entrust part of their IT operations to outsourcing companies. Even basic tasks, such as applying patches and configuring firewalls, can become the responsibility of the cloud service provider, not the user. This means that clients must establish trust relationships with their providers and understand the risk in terms of how these providers implement, deploy, and manage security on their behalf. This *trust but verify* relationship between cloud service providers and consumers is critical because the cloud service consumer is still ultimately responsible for compliance and protection of their critical data, even if that workload had moved to the cloud. In fact, some organizations choose private or hybrid models over public clouds because of the risks associated with outsourcing services.

Other aspects about cloud computing also require a major reassessment of security and risk. Inside the cloud, it is difficult to physically locate where data is stored. Security processes that were once visible are now hidden behind layers of abstraction. This lack of visibility can create a number of security and compliance issues.

In addition, the massive sharing of infrastructure with cloud computing creates a significant difference between cloud security and security in more traditional IT environments. Users spanning different corporations and trust levels often interact with the same set of computing resources. At the same time, workload balancing, changing service level agreements, and other aspects of today's dynamic IT environments create even more opportunities for misconfiguration, data compromise, and malicious conduct.

Infrastructure sharing calls for a high degree of standardized and process automation, which can help improve security by eliminating the risk of operator error and oversight. However, the risks inherent with a massively shared infrastructure mean that cloud computing models must still place a strong emphasis on isolation, identity, and compliance.

Cloud computing is available in several service models (and hybrids of these models). Each presents different levels of responsibility for security management. Figure 1 on page 3 depicts the different cloud computing models.

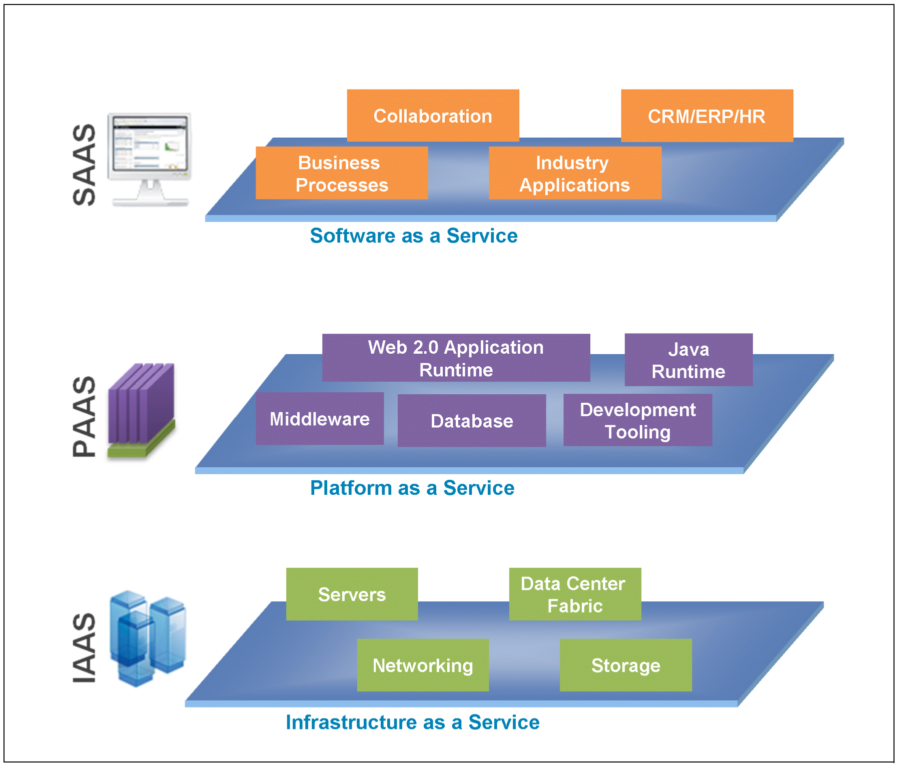

Figure 1 Cloud computing models

Evaluate different models of cloud computing

Different models of cloud computing have various ways of exposing their underlying infrastructure to the user. This influences the degree of direct control over the management of the computing infrastructure and the distribution of responsibilities for managing its security.

With the *Software as a Service* (SaaS) model, most of the responsibility for security management lies with the cloud provider. SaaS provides a number of ways to control access to the Web portal, such as the management of user identities, application level configuration, and the ability to restrict access to specific IP address ranges or geographies.

Cloud models like *Platform as a Service* allow clients to assume more responsibilities for managing the configuration and security for the middleware, database software, and application runtime environments. The *Infrastructure as a Service* (IaaS) model transfers even more control, and responsibility for security, from the cloud provider to the client. In this model, access is available to the operating system that supports virtual images, networking, and storage.

Organizations are intrigued with these cloud computing models because of their flexibility and cost-effectiveness, but they are also concerned about security. Recent cloud adoption studies by industry analysts and articles in the press have confirmed these concerns, citing the lack of visibility and control, concerns about the protection of sensitive information, and storage of regulated information in a shared, externally managed environment.

Note: A mass adoption of external, massively shared, and completely open cloud computing platforms for critical IT services is considered to be still a few years away.

In the near term, most organizations are looking at ways to leverage the services of external cloud providers. These clouds would be used primarily for workloads with a low-risk profile, where a one-size-fits-all approach to security with few assurances is acceptable, and where price is the main differentiator. For workloads with a medium-to-high-risk profile involving highly regulated or proprietary information, organizations are choosing private and hybrid clouds that provide a significant level of control and assurance. These workloads will be shifting into external clouds as they start offering tighter and more flexible security.

IBM provides a comprehensive framework for better understanding enterprise security. This framework is depicted in Figure 2. In the following section, we take a closer look at this framework to better understand the different aspects of a holistic security architecture.

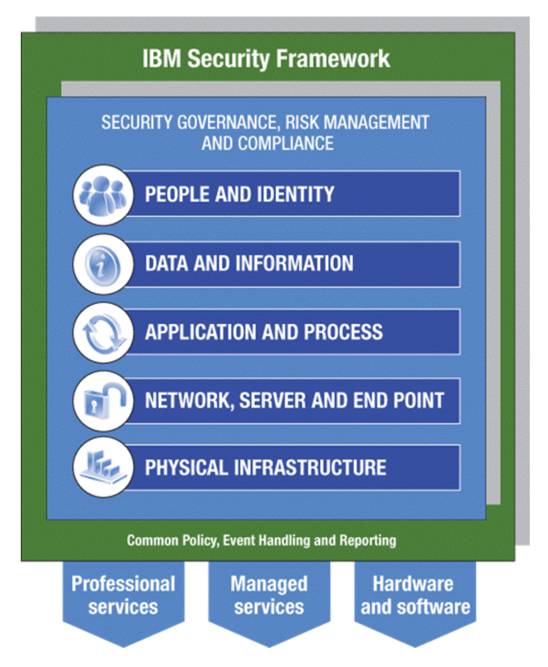

Figure 2 The IBM Security Framework

Examine the IBM Security Framework

The IBM Security Framework was developed to describe security in terms of the business resources that need to be protected, and it looks at the different resource domains from a business point of view.

Based on the IBM Security Framework and informed by extensive discussions with IBM clients, we provide a host of major security requirements in enterprise-class cloud computing today. (For more information, refer to the IBM Redguide™ *Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security*, REDP-4528.)

Security governance, risk management, and compliance

Organizations require visibility into the security posture of their cloud. This includes broad-based visibility into change, image, and incident management, as well as incident reporting for tenants and tenant-specific log and audit data.

Visibility can be especially critical for compliance. The Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), European privacy laws, and many other regulations require comprehensive auditing capabilities. Since public clouds are by definition a *black box* to the subscriber, potential cloud subscribers may not be able to demonstrate compliance. (A private or hybrid cloud, on the other hand, can be configured to meet those requirements.)

In addition, providers sometimes are required to support third-party audits, and their clients can be directed to support e-Discovery and forensic investigations when a breach is suspected. This adds even more importance to maintaining proper visibility into the cloud.

In general, organizations often cite the need for flexible Service Level Agreements (SLAs) that can be adapted to their specific situation, building on their experiences with strategic outsourcing and traditional, managed services.

People and identity

Organizations need to make sure that authorized users across their enterprise and supply chain have access to the data and tools that they need, when they need it, while blocking unauthorized access. Cloud environments usually support a large and diverse community of users, so these controls are even more critical. In addition, clouds introduce a new tier of privileged users: administrators working for the cloud provider. Privileged-user monitoring, including logging activities, becomes an important requirement. This monitoring should include physical monitoring and background checking.

Identity federation and rapid onboarding capabilities must be available to coordinate authentication and authorization with the enterprise back-end or third-party systems. A standards-based, single sign-on capability is required to simplify user logons for both internally hosted applications and the cloud, allowing users to easily and quickly leverage cloud services.

Data and information

Most organizations cite data protection as their most important security issue. Typical concerns include the way in which data is stored and accessed, compliance and audit requirements, and business issues involving the cost of data breaches, notification requirements, and damage to brand value. All sensitive or regulated data needs to be properly segregated on the cloud storage infrastructure, including archived data.

Encrypting and managing encryption keys of data in transit to the cloud or data at rest in the service provider's data center is critical to protecting data privacy and complying with compliance mandates. The encryption of mobile media and the ability to securely share those encryption keys between the cloud service provider and consumer is an important and often overlooked need. Because moving large volumes of data quickly and cheaply over the Internet is still not practical in many situations, many organizations must send mobile media, such as an archive tape, to the cloud provider. It is critical that the data is encrypted and only the cloud provider and consumer have access to the encryption keys.

Significant restrictions regarding data co-location can arise with cloud computing, depending on an organization's location, the type of data it handles, and the nature of its business. Several member states of the European Union (EU), for example, expressly forbid the nonpublic personal information of its citizens to leave their borders.

Note: A number of U.S. state governments do not allow the nonpublic personal information of its employees to be sent offshore.

Additionally, a cloud deployment can raise export-law violation issues relative to encrypted information, and the deployment can potentially expose intellectual property to serious threats. The organization's legal counsel must perform a thorough review of all these requirements prior to cloud deployment, making sure the organization can maintain control over the geographic location of data in the provider infrastructure.

In areas involving users and data with different risk classes that are explicitly identified (such as public and financial services), organizations need to maintain cloud-wide data classification. The classification of the data will govern who has access, how that data is encrypted and archived, and how technologies are used to prevent data loss.

Application and process

Clients typically consider cloud application security requirements in terms of image security. All of the typical application security requirements still apply to the applications in the cloud, but they also carry over to the images that host those applications. The cloud provider needs to follow and support a secure development process. In addition, cloud users demand support for image provenance and for licensing and usage control. Suspension and destruction of images must be performed carefully, ensuring that sensitive data contained in those images is not exposed.

Defining, verifying, and maintaining the security posture of images in regards to client-specific security policies is an important requirement, especially in highly regulated industries. Organizations need to ensure that the Web services they publish into the cloud are secure, compliant, and meet their business policies. Leveraging secure-development best practices is a key requirement.

Network, server, and endpoint

In the shared cloud environment, clients want to ensure that all tenant domains are properly isolated and that no possibility exists for data or transactions to leak from one tenant domain into the next. To help achieve this, clients need the ability to configure trusted virtual domains or policy-based security zones.

As data moves further from the client's control, they expect capabilities like Intrusion Detection and Prevention systems to be built into the environment. The concern is not only intrusions into a client's trusted virtual domain, but also the potential for data leakages and for *extrusions*, that is, the misuse of a client's domain to mount attacks on third parties. Moving data to external service providers raises additional concerns about internal and Internet-based denial of service (DoS) or distributed denial of service (DDoS) attacks.

Note: Because information security is a moving target, the environment must be reviewed on a regular basis against prevalent threats and common vulnerabilities.

In a shared environment, all parties must agree on their responsibilities to review data and perform these reviews on a regular basis. The organization must take the lead in terms of contract management for any risk assessments or controls deployment that it does not perform directly.

Where image catalogs are provided by the cloud provider, clients want these images to be secure and properly protected from corruption and abuse. Many clients expect these images to be cryptographically certified and protected.

Physical infrastructure

The cloud's infrastructure, including servers, routers, storage devices, power supplies, and other components that support operations, should be physically secure. Safeguards include the adequate control and monitoring of physical access using biometric access control measures and closed circuit television (CCTV) monitoring. Providers need to clearly explain how physical access is managed to the servers that host client workloads and that support client data.

Guide to implementing a secure cloud

The following security measures represent general best practice implementations for cloud security. At the same time, they are not intended to be interpreted as a guarantee of success. Please consult with your IBM security services representative to identify the best practice guidance for your specific implementation requirements.

- Implement and maintain a security program.
- Build and maintain a secure cloud infrastructure.
- Ensure confidential data protection.
- Implement strong access and identity management.
- Establish application and environment provisioning.
- Implement a governance and audit management program.
- Implement a vulnerability and intrusion management program.
- Maintain environment testing and validation.

Implement and maintain a security program

A security program can provide the structure for managing information security, and the risks and threats to the target environment. In the event of a security breach, the security program can provide crucial information as to how the cloud is protected, responses to threats, and a line of accountability for management of events.

1. **Security program implementation considerations.**

   When building a security program, the following recommendations should be taken into consideration:

   1.1. Evaluate and document the organization's culture as it relates to general security:

   a. Evaluate current industry and organization specific requirements in establishing best practices for secure infrastructure. For example, in the United States, organizations in the health care industry may qualify as covered entities under the Health Insurance Portability and Accountability Act (HIPAA).

   b. If trade secrets form the basis for a company's competitive advantage, the corporate security program must specify compliance requirements.

   c. If export controls apply to a company's data, it is important to address a specific compliance methodology for the data.

d. Evaluate each proposed cloud application for its appropriateness to cloud deployment. A careful discussion of a company's needs with the cloud provider or with the builder of the secure infrastructure may be helpful in evaluating whether and what type of cloud offering could work.

1.2. Prioritize the security attributes appropriate to your cloud implementation in order of importance.

1.3. Create and maintain policies and procedures relative to how the organization will address the various security considerations for clouds.

a. Policies should identify the threats to the cloud environment and its contents; they have to be maintained in order to address current threats.

b. The policy should identify key metrics to monitor and the frequency at which they should be evaluated; these metrics and measurements may be dictated by industry regulations or best practices.

c. The policy should specify a structure for accountability.

d. The policy should provide response recommendations in the case of an event.

e. Recommended responses should identify key actions, personnel, and escalation procedures within a specific time frame.

1.4. Work with the leadership or executive team responsible for the cloud implementation to ensure understanding and support of the initiative.

1.5. Implement an organization-wide education program to communicate the security policies and gain a general understanding of the policies.

a. Ensure that all persons with administrative roles complete required training activities.

b. Ensure that the policy is published in a location that is easily accessible by all those responsible for policy implementation and management.

1.6. Implement a system to ensure transparency of security status and anomalous events.

1.7. Establish an audit program.

1.8. Implement an enforcement model to ensure to allow for communication of events and accountability.

1.9. Create a notification program that communicates to appropriate personnel any anomalous events in as close to real time as reasonably possible.

Build and maintain a secure cloud infrastructure

A secure infrastructure helps provide cloud resiliency and the confidence that the information stored in the cloud is adequately protected. During the due diligence process, organizations must ensure that the vendor can meet all business requirements, demonstrates an understanding of all legal, regulatory, industry, and customer specific requirements, and has the capacity to meet those requirements in a satisfactory manner.

2. **Install and maintain a firewall configuration.**

A firewall configuration should be installed and maintained following the following recommendations:

2.1. Establish firewall configurations that include the following conditions:

a. A formal change management process for the firewall that results in formal approval and acceptance of configuration changes.

b. A firewall should be placed at each external network interface, and between each security zone within the cloud.

c. A diagram of network interfaces and locations that correlates to information flow and firewall placement, which must consider the activation of virtualized environments as well as soft firewall solutions.

d. A documented and maintained list of ports and services necessary for business operations and continuity. The default setting for firewall ports should be to deny access.

e. Justification and risk assessment for any firewall protocol exceptions or anomalous design definitions.

f. Description of groups, roles, and definitions for logical network management.

g. Quarterly assessment of firewall and router configurations and rule sets.

h. Standards for firewall configuration and router configuration.

2.2. Build and deploy a firewall that denies access from “untrusted” sources or applications, and adequately logs these events.

2.3. Build and deploy a firewall that restricts access from systems that have direct external connection and those which contain confidential data or configuration data. The configuration should include the following:

a. Specific restriction of traffic between specified filter ports and addresses.

b. Disallows direct access from external interfaces into the restricted network zones.

c. Implementation of dynamic packet filtering.

d. Restriction of all inbound and outbound traffic to that information specified in the documented and maintained list of ports and services.

e. Prevention of direct wireless access to the cloud infrastructure.

f. Prevention of internal address direct access to external interfaces.

2.4. Install perimeter firewalls between confidential and configuration data and external interfaces where supported by the cloud host.

2.5. Installation of personal firewall software, solutions on external devices, such as computers, mobile computers, mobile devices, and so on, that interface with the cloud environment where supported by your cloud host.

2.6. Implement IP masks to prevent internal systems from being presented and identified to external entities.

2.7. Implement a firewall to isolate confidential information, and ensure that all confidential information is stored behind the firewall.

3. **Do not use vendor supplied defaults for passwords and other security parameters.**

Vendor supplied defaults for security parameters, such as passwords, should not be used.

3.1. Always change vendor supplied passwords and security parameters before activating a server, or prior to the creation of virtual machine images.

3.2. Develop cloud configuration standards and guidelines for your organization. Document these standards and ensure that your cloud environment is in compliance. Ensure that these standards are consistent with industry hardening guidelines.

3.3. Ensure that each virtual machine implements only one primary function.

3.4. Ensure that no unnecessary functions or processes are active.

3.5. Remove all unnecessary applications, scripts, or modules form the virtual system.

4. **Protect administrative access.**

   All administrative access should be properly protected with access controls and secure networking.

   4.1. Use secure networking protocols for all administrative actions (SSH, SSL, IPSEC, and VPN), with bi-directional authentication.

   4.2. Require dual controls for all provider access to consumer resources (provider and consumer authentication and authorization for operations).

   4.3. Maintain am audit trail of administrative actions.

   4.4. The cloud host should develop and publish configuration management guidelines.

   4.5. Implement an Asset Discovery Mechanism to identify resources in use in the target environment.

   4.6. Regularly review Asset Maps to understand assets in the cloud environment.

   4.7. Maintain a Configuration Data Store to enable auditability and general security understanding.

5. **Ensure patch management.**

   The implementation of a patch management program should be ensured.

   5.1. The cloud host should develop and publish a patch and change management program.

   5.2. Develop a pre-production patch management system to enable business resiliency.

   5.3. Ensure logging is enabled for all patch processes, and develop the appropriate documentation.

   5.4. Ensure that all systems, and applications are running the latest vendor supplied patches, and updates within the specified period as specified in the patch and change management program. Ensure that an appropriate time frame is established.

   5.5. Establish a process or utilize a third-party vendor to maintain awareness of the latest security vulnerabilities.

6. **Implement a physical environment security plan.**

   A security plan for the physical environment should be implemented.

   6.1. Ensure that the facility has the appropriate physical security controls to prevent unauthorized access to critical areas within facilities and access to physical assets and systems by intruders or unauthorized users.

   6.2. Ensure that all employees with direct access to systems have full background checks.

   6.3. Ensure that all third-party providers have policies and procedures in place to distinguish employees from visitors.

   6.4. Ensure that the hosting service has adequate natural disaster protection.

7. **Protect hybrid communications.**

   Communications between the remote and corporate infrastructures should be properly protected.

   7.1. Ensure that access to the corporate infrastructure is only possible through secure communications.

7.2. Ensure that all communications between remote and corporate infrastructures are encrypted.

7.3. Ensure that communications can only originate from the corporate infrastructure.

7.4. Ensure that the corporate infrastructure is protected by a firewall.

7.5. Ensure that all communications between remote and corporate infrastructures can occur only over a dedicated network pipe.

7.6. Limit the number of users with administrative access to both corporation and remote infrastructures.

7.7. Make adequate provisions for protected out-of-band communications in the event of an emergency.

Ensure confidential data protection

Data protection is a core principle of information security. All of the prevalent information security regulations and standards, as well as the majority of industry best practices, require that sensitive information be adequately protected in order to preserve confidentiality. Confidentiality of such data is required no matter where that data is resident in the chain of custody, including the cloud environment.

8. Protect Personally Identifiable Information (PII).

PII should be carefully handled and protected.

8.1. Develop and publish rules for the origination, capture, handling, transmission, storage, and disposal of PII data.

8.2. Consult with a legal advisor for requirements applicable to you/your industry.

8.3. Develop a PII Breach Policy notification strategy and policy for communication of breach information, in accordance with national, state, and Federal law, and industry regulation and best practices.

8.4. Develop a PII data inventory and classification schema.

8.5. Keep PII information storage to a minimum by adopting the following policies:

a. Develop and implement a data retention policy.

b. Securely destroy all non-essential PII data (*regulatory requirements may apply*).

9. Securely destroy all non-essential PII.

PII information not essential to the business should be securely destroyed.

9.1. Mask displayed PII information when appropriate (for example, display subset of Social Security Numbers).

9.2. Render PII Information unreadable whenever stored.

9.3. Ensure that PII information in memory is unreadable and un-addressable by client technologies.

9.4. Ensure that PII information is not recorded in log files or other system files.

9.5. Ensure logging of all PII information extracts occurs to mitigate data leakage.

10. Protect confidential and business critical data.

Develop and implement a policy to protect confidential and business critical data.

10.1. Develop and publish rules for the origination, capture, handling, transmission, storage, and disposal of confidential data.

10.2. Develop a PII breach policy notification strategy and policy for communication of breach information, in accordance with national, state, and Federal law, and industry regulation and best practices.

10.3. Develop and maintain a confidential data inventory and classification schema.

10.4. Keep confidential information storage to a minimum by adopting the following policies:

a. Develop and implement a data retention policy.

b. Securely destroy all non-essential confidential information (*regulatory requirements may apply*).

10.5. Perform an assessment of data impact before deploying the data to the cloud, which should consist of documenting and assessing risk tolerance.

10.6. Do not permit storage of sensitive information prior to authentication of the user.

11. Protect intellectual property.

Develop and implement a policy to protect intellectual property.

11.1. Prior to any public cloud deployment, the organization's risk assessment should include intellectual property that may be exposed.

11.2. When using a public cloud, the organizations' general counsel should ensure that SLA agreements cover the protection of intellectual property.

11.3. When deploying to a public cloud, organizations should attempt to obscure intellectual property as much as possible through encryption, or other mechanisms, which create difficulty for malicious users to reverse-engineer the information.

12. Protect encryption keys from misuse or disclosure.

Ensure that encryption keys are securely managed to prevent misuse or disclosure.

12.1. Fully document and implement a key storage management program, inclusive of the following topics:

a. Generation of minimum key strength guidelines and policies.

b. A secure key distribution and management methodology.

c. Periodic recycling of keys annually, at minimum.

d. A methodology for destruction of old or inactive keys.

e. A mechanism to ensure prompt disposal and replacement of suspected compromised keys.

f. A process for notification of suspected compromised key events.

g. Prevent the unauthorized substitution of keys.

h. Split-knowledge and establishment of dual control of keys.

i. Rules regarding record information must be documented and appropriate archival mechanisms must be put in place.

12.2. Implement a key management program:

a. Apply the principle of least-privilege when granting access to keys.

b. Regularly review user access rights to keys.

c. Store keys in as few a places as possible.

d. Log all access to keys.

13. Secure data communications.

Implement a secure data communications policy.

13.1. Document and publish guidance for the means and requirements of data communication.

13.2. Utilize strong cryptography and security protocols, such as SSL/TLS and IPSEC, to protect sensitive information.

13.3. Never send unencrypted PII or confidential information by e-mail.

13.4. Use a secure network protocol when connecting to a secure information store.

13.5. Ensure that when archives are being created and that secure transports are utilized.

14. Implement data loss prevention.

Implement a data loss prevention (DLP) mechanism to prevent data leakage.

14.1. Implement a DLP mechanism to prevent accidental or intentional leakage of information.

14.2. Ensure that the DLP mechanisms provide appropriate reporting.

14.3. Ensure that your DLP solution is integrated with security policies.

15. Protect application information.

Ensure that applications are protecting the information that they are processing.

15.1. Implement a code review of all client code that manipulates personal or sensitive data, and document the types of information stored.

15.2. Ensure that all PII or confidential information is stored in an unreadable format.

15.3. Ensure that any PII or sensitive information stored in cookies is encrypted and in an unreadable format.

15.4. Prevent routine storage of encryption keys in local systems.

15.5. Prevent the caching of PII or sensitive Information.

15.6. When displaying PII or sensitive information, ensure that masking is implemented for fields that display data.

15.7. Do not allow storage of sensitive data as constant variables in the application.

15.8. Regularly scan Web applications for vulnerabilities.

Implement strong access and identity management

Access and identity management are critical to cloud security. They limit access to data and applications to authorized and appropriate users.

16. Implement a least privilege model.

Ensure that users' access privileges are appropriate, and that secure access mechanisms are in place.

16.1. Regularly evaluate the users' access list to ensure that only appropriate levels of access are granted, and only personnel with an authorized need have access to systems.

16.2. Establish a policy for systems that have multiple users, restricting access based on need-to-know.

16.3. Ensure that systems verify and check the identity of all users against an approved access list prior to granting access.

16.4. Ensure that an approved authentication mechanism is in place.

16.5. Implement multi-factor authentication access to all systems and administrative systems.

16.6. For access to administrative functions, implement technologies such as dial-in and remote authentication VPN (SSL/TLS and IPSEC) with individual certificates.

16.7. Encrypt all passwords during transmission and storage.

16.8. To ensure that proper authentication and password management functions on all system elements, utilize the following as guidelines:

a. Control management of user ID credentials and other ID information.

b. Verify a user identity prior to password change or reset.

c. Require that users change their password upon first entry into the application.

d. Promptly revoke access for terminated users.

e. Remove inactive accounts at least every 30 days.

f. Ensure documentation of password and ID policies, and train employees in guidelines.

g. Ensure that contractor and hosting passwords are only enabled during maintenance schedules.

h. Do not allow group, shared, or generic accounts or passwords.

i. Require users to change passwords at predefined interval (30, 60, or 90) days.

j. Require complex passwords for users that contain alpha and numeric characters.

k. Limit password reuse to a prescribed number (for example, disallow reuse of the last 3 passwords).

l. Limit the number of failed password attempts a user may attempt prior to being locked out of a system.

m.Set an inactive expiration period for all systems in cases where confidential data requires a user to re-authenticate to the system.

n. Apply a lockout rule that either has a time constraint, or requires re-activation as a service function.

17.Implement federated identity management.

Identity federation should be deployed to securely exchange identity information.

17.1. Ensure that a federated identity management is implemented when bridging cloud environments.

17.2. Ensure that when federating identities a system of identity confidence is implemented to prevent identity spoofing.

Establish application and environment provisioning

In a centrally managed cloud environment, it is essential to have automated provisioning functionality in place.

18.Implement a program for application provisioning.

Design and implement a program for provisioning images and applications.

18.1. Ensure that an approved process for provisioning virtual images is in place.

18.2. Ensure that the provisioning system applies access rights at the time of provisioning.

18.3. Ensure that the provisioning management has the appropriate security and authorization controls.

18.4. Ensure that application and virtual image de-provisioning activities are logged.

18.5. Ensure that all changes to access of virtual images and applications are logged.

18.6. Regularly review provisioning management system access to ensure that only least privileged access rules are enforced.

18.7. Ensure that a mechanism is in place that governs destruction of outdated or invalid virtual images.

Implement a governance and audit management program

To be prepared for regulatory or internal audits, you need to have a program in place that defines when, how, and where to collect log and audit information.

19. Implement a privacy management program.

19.1. Implement a privacy management program with the following attributes:

a. Create an understanding of what PII and business confidential information exists and is managed.

b. Prioritize PII and confidential information relative to risk and regulatory impacts.

c. Write policies on usage, retention, modification, and deletion of PII and confidential data.

d. Work with executive and leadership teams to validate the program.

e. Implement a process for monitoring policy compliance and exceptions.

f. Create an education program relative to the policy.

g. Create an audit program for policies.

h. Create rules for the enforcement and monitoring of policy.

i. Create a program/process for notification of the appropriate parties in the event of a breach.

19.2. Add PII data to the data reference map to allow auditors and administrators to identify threats to the cloud environment.

20. Implement mechanisms for audit capture and management.

Implement an audit management and records management program.

20.1. Work with your legal counsel to identify and document all applicable legal and regulatory requirements for each cloud instance.

20.2. Based on the above, create policies for the capture and retention of legal and regulatory documents.

20.3. Implement a regular review of retained information.

20.4. Implement an audit program to ensure that audit capture and retention policies are enforced.

20.5. Ensure the collection of all legal and regulatory documents as required.

21. Document cross border protection and compliance.

Document, review, and enforce policies that ensure that data is handled and stored in compliance with regulations and cross-border protection requirements.

21.1. All applicable regional, national, and international laws should be reviewed with your legal counsel to understand the requirements related to the transfer and utilization of storage by cloud consumers and hosts.

21.2. Document policies and procedures relative to those international, national, and regional laws and regulations that affect the business, including:

a. Where data must be stored based on content and data consumer.

b. Who has access to data based on content and data consumer.

c. What protections (encryption, segregation, and so on) must be put in place to protect data based on the aforementioned regional, national, and international laws or regulations that affect the business.

21.3. Regularly review the various regulation and laws with your legal counsel that may apply to the creation, storage, transmission, and destruction of data as it relates to cross-border protections.

21.4. Ensure that in cases where consent is required, a record is maintained to confirm that they data subject has provided said consent.

21.5. Ensure that data processors are aware of the activities and constraints that are applicable with regard to the sensitive information.

Implement a vulnerability and intrusion management program

In a trusted cloud environment, you have to implement a strict vulnerability management program and mechanisms such as intrusion detection systems (IDS) and intrusion prevention systems (IPS) to ensure that IT resources (servers, network, infrastructure components, and endpoints) are constantly monitored for vulnerabilities and breaches.

22. Implement and regularly update antivirus/anti-spyware and IDS/IPS.

Vulnerability scanning, antivirus, and intrusion detection and prevention mechanisms must be deployed to protect the environment.

22.1. Deploy antivirus software on all supported systems that could be exposed to virus or spyware attacks.

22.2. Ensure that selected programs can identify, isolate, or remove, and protect against malicious software or processes.

22.3. Develop policies for machine classifications relative to antivirus management protocols.

22.4. Ensure that all protection mechanisms are current and actively running, and capable of generating logs.

22.5. Use network and host-based intrusion-detection or intrusion prevention systems to monitor activity in the cloud environment and alert personnel to suspected compromises.

22.6. Keep all intrusion-detection and prevention engines up-to-date.

a. Verify the use of intrusion-detection systems or intrusion-prevention systems and that all traffic in the cloud environment is monitored.

b. Confirm that IDS or IPS are configured to alert personnel of suspected compromises.

Maintain environment testing and validation

In order to maintain an intact cloud IT environment, you have to employ different mechanisms for testing and validation.

23. **Implement a change management process.**

    Document and implement a change management process.

    23.1. Ensure that there is a documented configuration change management process in place.

    23.2. Follow a configuration change management process for systems and software within the cloud. It should include the following:

    a. Change request logging.

    b. Impact assessment statement.

    c. Pre-production test results and sign-off.

    d. Process for roll back to a prior state.

24. **Implement a data encryption and access program.**

    Implement a program to test that stored data is properly protected.

    24.1. Test databases and other storage mediums to ensure that they are adequately protected, and the proper encryption levels are applied.

25. **Implement a program for secure application development and testing.**

    A secure application development and testing program should be implemented.

    25.1. Develop software applications based on best practices, with security being a conscious component of the initiative.

    a. Validation of all security patches prior to production deployment.

    b. Ensure that test and production environments are separate.

    c. Ensure separation of duties between test, development, and administration personnel.

    d. Do not use production data that contains confidential or PII information in a test environment.

    e. Ensure removal of all test data and administrative information from the test environment prior to conversion to production.

    f. Ensure that all test accounts and custom accounts have been removed prior to production activation.

    g. Perform security code reviews on all code prior to release into production.

    25.2. Develop all Web based applications using secure coding guidelines, such as those provided by IBM, the Open Web Application Security Project, and so on. Regularly review code for common security vulnerabilities. Include the following:

    a. Un-validated inputs.

    b. Broken or ineffective access controls.

    c. Broken or ineffective authentication and session management.

    d. Cross site scripting vulnerabilities.

    e. Buffer overflow vulnerabilities.

    f. Injection-based vulnerabilities, such as SQL, LDAP, and so on.

    g. Improper or non-existent error handling.

h. Insecure storage methods or technologies.

i. Insecure configuration management.

j. Susceptibility to denial of service attacks.

25.3. Ensure that trace and debug statements are removed from production code.

25.4. Ensure that the application does not have name enumeration errors.

25.5. Ensure that all Web facing applications are protected against known attacks by one of the following mechanisms:

a. Installation of an application firewall.

b. Have a reliable third party review the application for security vulnerabilities.

25.6. Implement a program for network monitoring and testing.

25.7. Ensure that a process is in place that associates each unique ID with all activity, especially those activities that relate to administrative activities.

25.8. Ensure that audit trails are enabled for all events, especially the following events:

a. Invalid login attempts.

b. Any administrative access attempts.

c. All events involving access to confidential or PII data.

d. Any access to systems functions or audit trails.

e. Activation or cessation of system functions or processes.

f. All administrative activities.

g. Any activation or cessation of virtual systems.

25.9. Record the following information at a bare minimum:

a. User ID.

b. Time of event.

c. Event description.

d. Event origin, if appropriate.

e. Event success or failure.

f. Affected entity.

25.10. Ensure that all audit trails are secured.

25.11. Limit access to administrative functions.

25.12. If possible, encrypt audit trails.

25.13. Ensure that audit trails are regularly backed up.

25.14. Use file monitoring and alteration detection to determine unauthorized changes to files.

25.15. Ensure that clocks are synchronized.

25.16. Retain audit trail history for at least a year, or according to applicable regulatory requirements.

25.17. Test security controls for validity by leveraging tools for verifying endpoints against threats.

25.18. Test applications prior to deployment by leveraging commercial application and service validation tools.

25.19. Perform penetration testing at least once every 90 days to determine if vulnerabilities have been introduced into your cloud environment.

25.20. Deploy file integrity monitoring solutions to identify the introduction of malicious code.

Summary

Cloud computing provides an efficient, scalable, and cost-effective way for today's organizations to deliver business or consumer IT services over the Internet. A variety of different cloud computing models are available, providing both solid support for core business functions and the flexibility to deliver new services.

However, the flexibility and openness of cloud computing models have created a number of security concerns. Massive amounts of IT resources are shared among many users, and security processes are often hidden behind layers of abstraction. More to the point, cloud computing is often provided as a service, so control over data and operations is shifted to third-party service providers, requiring their clients to establish trust relationships with their providers and develop security solutions that take this relationship into account.

In this paper, we presented guidance on cloud computing security. We examined the major security challenges for cloud providers and their clients, and we discussed concrete guidelines for the implementation of cloud security controls that are based on recognized security frameworks and industry best practices.

The team that wrote this IBM Redpapers publication

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization, Austin Center.

Axel Buecker is a Certified Consulting Software IT Specialist at the International Technical Support Organization, Austin Center. He writes extensively and teaches IBM classes worldwide on areas of Software Security Architecture and Network Computing Technologies. He holds a degree in Computer Science from the University of Bremen, Germany. He has 23 years of experience in a variety of areas related to Workstation and Systems Management, Network Computing, and e-business Solutions. Before joining the ITSO in March 2000, Axel worked for IBM in Germany as a Senior IT Specialist in Software Security Architecture.

Koos Lodewijkx is a portfolio manager in the IBM Corporate Security Strategy team, where he is responsible for the coordination of security strategy development across the IBM brands. He joined IBM in February 2007 when IBM acquired Consul risk management, a leader in the compliance management solution development and delivery industry. While at Consul, Koos held various management positions, and was product manager of Consul's audit and compliance reporting product line.

Harold Moss is an Emerging Technologies Architect with the IBM Corporate Security Strategy Team. He is responsible for providing technical insights into emerging security technology directions, as well as existing ones. He was responsible for verifying and validating architectural direction in a number of cloud and Web 2.0 based solutions, which ensured alignment with customer needs and other IBM assets. Currently, Harold sits on several IBM architecture boards and champions the delivery of assets for cloud computing and Web 2.0 technologies.

Kevin Skapinetz is the portfolio manager for SaaS security at IBM Internet Security Systems. In this position, he is responsible for defining and executing the strategic direction for IBM security-as-a-service offerings. With 10 years of experience in information security and 7 years at ISS, Kevin has held variety of important positions in strategy, engineering, and support. He recently played a central role in the Office of the CTO as a technology strategist, where he guided the company's strategy for emerging technologies, including secure virtualization and secure cloud computing. He also spent several years as the lead software engineer for RealSecure Server Sensor, a multi-platform host intrusion prevention system. Kevin holds a degree in Computer Science degree from Tulane University and a Master degree in Information Security from the Georgia Institute of Technology.

Michael Waidner received a Doctorate (PhD) in Computer Science from the University of Karlsruhe, Germany, in 1991. In 1994, after a few years as researcher and lecturer at the University of Karlsruhe, he joined IBM Research in Rüschlikon, Switzerland, where he formed and led one of the most successful industrial security research teams worldwide. Under his leadership, the team made numerous fundamental contributions to science and IBM's product and services portfolio, in areas such as cryptography, fault tolerance in distributed systems, federated identity management, enterprise privacy management, security governance, and risk management. In 2006, he moved from Switzerland to the US, and joined the IBM Software Group in New York. In 2007, he led the creation of the IBM Security Architecture Board, which has cross-IBM responsibility for architecture and technical strategy in security. Michael has been chairing this board since the beginning, and established it as the core of the virtual cross-IBM security technology organization. Michael has authored or co-authored more than 110 scientific publications. He is a member of the IBM Academy of Technology, a Fellow of the IEEE, and an ACM Distinguished Scientist.

Thanks to the following people for their contributions to this project:

Wade Wallace
International Technical Support Organization, Austin Center

Calvin Powers, Steven Bade, Marne Gordan, Latha Maripuri, Mari Heiser, Harriet Pearson, Ellen Dulburger, Stephen Mortinger, Tony Nadalin, Ana Lacovetta, Ayomi Burge, Anna Coffey, Annette Miller, David Boloker, Adi Sharabani, Mary Ellen Zurko, Kristof Klockner, Kristin Lovejoy, Christopher Bauserman, Omkhar Arasaratnam, Heather Hinton, Steve Wojtowecz, **IBM**

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document REDP-4614-00 was created or updated on November 2, 2009.

Send us your comments in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:
  ibm.com/redbooks
- Send your comments in an email to:
  redbooks@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

Trademarks